STIC Search Report
EIC 2100

STIC Database Tracking Number: 120549

TO:	From:
Kambiz Zand **Location: 4C10** **Art Unit : 2132** **Friday, April 30, 2004** **Case Serial Number: 09/599005**	**David Holloway** **Location: EIC 2100** **PK2-4B30** **Phone: 308-7794** **david.holloway@uspto.gov**

Search Notes

Dear Examiner Zand,

Attached please find your search results for above-referenced case.
Please contact me if you have any questions or would like a re-focused search.

David

Access DB# 120549

117

SEARCH REQUEST FORM

Scientific and Technical Information Center

Requester's Full Name: Kambiz Zand Examiner #: 78582 Date: 04/27/04
Art Unit: 2132 Phone Number 306-4169 Serial Number: 09/599005
Mail Box and Bldg/Room Location: CPK2-4C10 Results Format Preferred (circle): PAPER DISK E-MAIL

If more than one search is submitted, please prioritize searches in order of need.

****

Please provide a detailed statement of the search topic, and describe as specifically as possible the subject matter to be searched. Include the elected species or structures, keywords, synonyms, acronyms, and registry numbers, and combine with the concept or utility of the invention. Define any terms that may have a special meaning. Give examples or relevant citations, authors, etc, if known. Please attach a copy of the cover sheet, pertinent claims, and abstract.

Title of Invention: Information Processing Device, Card device & information Processing Center.

Inventors (please provide full names): ~~Masahiro~~ Kaminaga; Takashi Endo; Masaru Ohki; Takashi Tsukamoto; Hiroshi Watase; Chiaki Terauchi; Kunihiko Nakada; Nobutaka Nagasaki; Satoshi Taira; Yuuichirou Namyoshi & Yasuke Ei Kitaiwa

Earliest Priority Filing Date: 6/24/1999

For Sequence Searches Only *Please include all pertinent information (parent, child, divisional, or issued patent numbers) along with the appropriate serial number.*

See enclosed papers

****

STAFF USE ONLY	Type of Search		Vendors and cost where applicable	
Searcher: David Wallace	NA Sequence (#)		STN	
Searcher Phone #: 308-7794	AA Sequence (#)		Dialog	$12.32 07/10
Searcher Location: CPK2 4B30	Structure (#)		Questel/Orbit	
Date Searcher Picked Up: 4-30-04	Bibliographic	✓	Dr.Link	
Date Completed: 4-30-04	Litigation		Lexis/Nexis	
Searcher Prep & Review Time: 65	Fulltext		Sequence Systems	
Clerical Prep Time:	Patent Family		WWW/Internet	✓
Online Time: 200	Other		Other (specify)	

PTO-1590 (8-01)

```
Set     Items   Description
S1        408   SMARTCARD? OR CHIPCARD? OR ICCARD? OR MONDEX? OR PHYSICAL(-
              )TOKEN? OR (SMART OR CHIP OR IC)()CARD? ?
S2      22959   POWER? OR VOLTAGE? OR AMP OR AMPS OR AMPERE? OR WATT? ? OR
              CURRENT?
S3        464   S2(2N)(CONTROL? OR FLUCTUAT? OR CHANG? OR VARY OR VARIES OR
               CHANG? OR MODERATE OR MEASUR? OR MONITOR?)
S4        249   S1(15N)(ENCRYPT? OR CRYPTO? OR SECUR? OR SAFE? OR DES OR R-
              SA OR PROTECT? OR ENCIPHER? OR ENCYPHER? OR SPA OR TA OR ATTA-
              CK? OR DPA)
S5          2   S3 (S) S4
S6          3   S3 (S) S1
S7          0   S6 (S) (LINE? OR BUS OR BUSSES OR PATH OR PATHS OR ROUTE OR
               ROUTES OR WIRE OR WIRES)
S8          0   S1(5N)(SPA OR TA OR DPA OR SIMPLE()POWER()ANALYSIS OR DIFF-
               ERENTIAL()POWER()ANALYSIS OR TIMING()ATTACK?)
S9          1   S3(5N)S4
S10         1   S9 OR S7
S11         2   S3 AND S4
S12         3   S6 OR S11
File 256:SoftBase:Reviews,Companies&Prods. 82-2004/Mar
         (c)2004 Info.Sources Inc
```

```
Set     Items   Description
S1      30973   SMARTCARD? OR CHIPCARD? OR ICCARD? OR MONDEX? OR PHYSICAL(-
             )TOKEN? OR (SMART OR CHIP OR IC)()CARD? ?
S2    2900693   POWER? OR VOLTAGE? OR AMP OR AMPS OR AMPERE? OR WATT? ? OR
             CURRENT?
S3     384258   S2(2N)(CONTROL? OR FLUCTUAT? OR CHANG? OR VARY OR VARIES OR
              MODERATE OR MEASUR? OR MONITOR?)
S4    2001956   ENCRYPT? OR CRYPTO? OR SECUR? OR SAFE? OR DES OR RSA OR KE-
             Y? ? OR PROTECT? OR ENCIPHER? OR ENCYPHER? OR ATTACK? OR SPA -
             OR TA OR DPA
S5        130   S1 AND S3 AND S4
S6         17   S5 AND IC=(G06F-015/16 OR G06F-012/14 OR G06F-007/10)
S7         52   S5 AND MC=(T01-D01 OR T01-F05B3 OR T01-H01B3A OR T01-H01C2
             OR T01-J12C OR T04-K02 OR T05-H02C5C OR U21-C02)
S8       4005   S1(10N)(S3 OR S4)
S9         34   S7 AND S8
S10        41   S6 OR S9
S11        41   IDPAT (sorted in duplicate/non-duplicate order)
S12        41   IDPAT (primary/non-duplicate records only)
S13        39   S5 AND (LINE? OR BUS OR BUSSES OR WIRE? OR CONNECTION? OR -
             PATH? OR ROUTE?)
S14        28   S13 NOT S11
S15         6   S14 AND IC=(G06F? OR H04K?)
S16         6   IDPAT (sorted in duplicate/non-duplicate order)
S17         6   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2003/Dec(Updated 040402)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200427
         (c) 2004  Thomson Derwent
```

17/5/1 **(Item 1 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

014587286 **Image available**
WPI Acc No: 2002-407990/200244
XRPX Acc No: N02-320502

Method for disguising the electrical power consumption of an integrated circuit during execution of a confidential operation by activating a charge pump so that any power variations due to the confidential actions are masked

Patent Assignee: STMICROELECTRONICS SA (SGSA); STMICROELECTRONICS (SGSA)
Inventor: WUIDART S
Number of Countries: 022 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2813972	A1	20020315	FR 200011696	A	20000914	200244	B
WO 200223312	A1	20020321	WO 2001FR2796	A	20010910	200244	
EP 1317701	A1	20030611	EP 2001967463	A	20010910	200339	
			WO 2001FR2796	A	20010910		
US 20030219126	A1	20031127	WO 2001FR2796	A	20010910	200378	N
			US 2003388324	A	20030312		

Priority Applications (No Type Date): FR 200011696 A 20000914; US 2003388324 A 20030312
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2813972	A1		17	G06K-019/073	
WO 200223312	A1	F		G06F-001/00	
Designated States (National): JP US					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR					
EP 1317701	A1	F		G06F-001/00	Based on patent WO 200223312
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR					
US 20030219126	A1			H04N-007/167	Cont of application WO 2001FR2796

Abstract (Basic): FR 2813972 A1

NOVELTY - During a confidential operation such as reading confidential data stored in the integrated circuit or calculation of a **cryptographic** code, a charge pump is activated such that it generates **fluctuations** in the **power** supply **line** to the integrated circuit, such that any power variations due to the confidential operations are masked.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is made for an integrated circuit with a device (CPU) capable of activating a charge pump such that the power consumption during confidential operations is masked.

USE - Prevention of fraud, particularly relating to **chip cards** .

ADVANTAGE - Invention provides a simple and effective method for thwarting fraud attempts made using power analysis.

DESCRIPTION OF DRAWING(S) - Figure show a circuit according to the invention.

integrated circuit. (10)

pp; 17 DwgNo 2/5

Title Terms: METHOD; DISGUISE; ELECTRIC; POWER; CONSUME; INTEGRATE; CIRCUIT ; EXECUTE; CONFIDE; OPERATE; ACTIVATE; CHARGE; PUMP; SO; POWER; VARIATION ; CONFIDE; ACTION; MASK
Derwent Class: T04; U24; W01
International Patent Class (Main): **G06F-001/00** ; G06K-019/073; H04N-007/167
International Patent Class (Additional): H04L-009/06; H04L-009/32
File Segment: EPI

```
Set     Items   Description
S1        155   AU=(KAMINAGA M? OR KAMINAGA, M?)
S2       5682   AU=(ENDO T? OR ENDO, T?)
S3        626   AU=(OHKI M? OR OHKI, M?)
S4       1970   AU=(TSUKAMOTO T? OR TSUKAMOTO, T?)
S5         13   AU=(WATASE H? OR WATASE, H?)
S6          4   AU=(TERAUCHI C? OR TERAUCHI, C?)
S7        547   AU=(NAKADA K? OR NAKADA, K?)
S8         22   AU=(NAGASAKI N? OR NAGASAKI, N?)
S9        373   AU=(TAIRA S? OR TAIRA, S?)
S10         6   AU=(NARIYOSHI Y? OR NARIYOSHI, Y?)
S11       276   AU=(FUKUZAWA Y? OR FUKUZAWA, Y?)
S12         0   S1 AND S2 AND S3 AND S4 AND S5 AND S6 AND S7 AND S8 AND S9
              AND S10 AND S11
S13     68508   SMARTCARD? OR (CHIP OR SMART OR IC OR PCMCIA)()(CARD OR CA-
              RDS) OR CHIPCARD? OR ICCARD? OR MONDEX
S14         2   S13 AND (S1:S11)
S15         1   S14 AND (POWER? OR WATT? OR VOLT? OR ELECTRICIT?)
S16         0   S14 AND (SENSE()AMPLIFIER?)
S17         1   S12 OR (S15 OR S16)
File   2:INSPEC 1969-2004/Apr W3
         (c) 2004 Institution of Electrical Engineers
File   6:NTIS 1964-2004/Apr W4
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2004/Apr W3
         (c) 2004 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Apr W4
         (c) 2004 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2004/Apr
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Apr W4
         (c) 2004 BLDSC all rts. reserv.
File  95:TEME-Technology & Management 1989-2004/Apr W2
         (c) 2004 FIZ TECHNIK
File 148:Gale Group Trade & Industry DB 1976-2004/Apr 30
         (c)2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2004/Apr 30
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Apr 30
         (c) 2004 The Gale Group
File 647:CMP  Computer Fulltext 1988-2004/Apr W3
         (c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Apr W3
         (c) 2004 IDG Communications
```

14/3,K/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

7270113 INSPEC Abstract Number: B2002-06-1265D-052, C2002-06-5320M-002
Title: Sensing technology for low-voltage operation FRAM
Author(s): **Endo, T.** ; Yamamoto, A.; Kawashima, S.
Journal: Fujitsu vol.53, no.2 p.100-4
Publisher: Fujitsu,
Publication Date: 2002 Country of Publication: Japan
CODEN: FUJTAR ISSN: 0016-2515
SICI: 0016-2515(2002)53:2L.100:STVO;1-N
Material Identity Number: D926-2002-002
Language: Japanese
Subfile: B C

Author(s): **Endo, T.** ; Yamamoto, A.; Kawashima, S.
Abstract: The important requirements for **smart card** LSI chips are low power consumption, nonvolatile storage, and high-speed rewrite operation to reduce processing time. A **smart card** is an **IC card** that contains a microcomputer, storage circuit, and RF circuit. The ferroelectric RAM (FRAM) has been...
...Descriptors: **smart cards**
...Identifiers: **smart card** LSI chips

14/3,K/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

5598297 INSPEC Abstract Number: C9707-5130-009
Title: Smart card **microprocessors for electronic money systems**
Author(s): Sato, T.; Tanaka, T.; **Nakada, K.** ; Takeshima, M.
Journal: Hitachi Review vol.46, no.1 p.31-6
Publisher: Hitachi,
Publication Date: Feb. 1997 Country of Publication: Japan
CODEN: HITAAQ ISSN: 0018-277X
SICI: 0018-277X(199702)46:1L.31:SCME;1-8
Material Identity Number: H006-97003
Language: English
Subfile: C

Title: Smart card **microprocessors for electronic money systems**
Author(s): Sato, T.; Tanaka, T.; **Nakada, K.** ; Takeshima, M.
Abstract: **Smart cards** , which are formed by embedding a semiconductor chip in a thin plastic card, are fast...

...cards. This technology features large data storage capability and a high level of data security. **Smart cards** are indispensable when implementing electronic settlement systems using electronic money, and have an important role...

... economic media that can be a substitute for cash value. This work will describe the **Mondex** electronic cash system in which Hitachi Ltd. is a key participant. The microprocessor used for...

... various functions, including large capacity data storage and a particularly high level of data security. **Mondex** will form the basis for future electronic settlement systems. In addition, it is becoming clear that **smart cards** technology will become widely used in the area of credit cards. Hitachi has developed a variety of microcomputers for **smart cards** and is rapidly becoming a leading company in this field.
...Descriptors: **smart cards**
Identifiers: **smart card** microprocessors...

... Mondex -;

```
Set     Items   Description
S1        286   AU=(KAMINAGA M? OR KAMINAGA, M?)
S2       8466   AU=(ENDO T? OR ENDO, T?)
S3        203   AU=(OHKI M? OR OHKI, M?)
S4       2457   AU=(TSUKAMOTO T? OR TSUKAMOTO, T?)
S5        131   AU=(WATASE H? OR WATASE, H?)
S6         17   AU=(TERAUCHI C? OR TERAUCHI, C?)
S7       3826   AU=(NAKADA K? OR NAKADA, K?)
S8        143   AU=(NAGASAKI N? OR NAGASAKI, N?)
S9        505   AU=(TAIRA S? OR TAIRA, S?)
S10        19   AU=(NARIYOSHI Y? OR NARIYOSHI, Y?)
S11       323   AU=(FUKUZAWA Y? OR FUKUZAWA, Y?)
S12         2   S1 AND S2 AND S3 AND S4 AND S5 AND S6 AND S7 AND S8 AND S9
              AND S10 AND S11
S13     48871   SMARTCARD? OR (CHIP OR SMART OR IC OR PCMCIA)()(CARD OR CA-
              RDS) OR CHIPCARD? OR ICCARD? OR MONDEX
S14       125   S13 AND (S1:S11)
S15        39   S14 AND (POWER? OR WATT? OR VOLT? OR ELECTRICIT?)
S16         1   S14 AND (SENSE()AMPLIFIER?)
S17        39   S12 OR (S15 OR S16)
S18        39   IDPAT (sorted in duplicate/non-duplicate order)
S19        33   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2003/Dec(Updated 040402)
         (c) 2004 JPO & JAPIO
File 348:EUROPEAN PATENTS 1978-2004/Apr W02
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040415,UT=20040408
         (c) 2004 WIPO/Univentio
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200427
         (c) 2004  Thomson Derwent
```

19/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016111074 **Image available**
WPI Acc No: 2004-268950/200425
XRPX Acc No: N04-212754

Memory accessing method for e.g. mobile phone, involves accessing memory portions associated with respective hamming distances, such that difference between distances is not more than predefined value

Patent Assignee: HITACHI LTD (HITA)
Inventor: **ENDO T** ; **KAMINAGA M** ; WATANABE T

Number of Countries: 032 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20040064715	A1	20040401	US 2003452138	A	20030603	200425	B
EP 1406145	A2	20040407	EP 200313398	A	20030618	200425	

Priority Applications (No Type Date): JP 2002288204 A 20021001
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040064715	A1		19	G06F-012/14	
EP 1406145	A2	E		G06F-001/00	

Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Abstract (Basic): US 20040064715 A1

NOVELTY - The move instructions, conditional branch and jump instructions which have specific program counter starting address are executed. The memory portions associated with respective hamming distances, are accessed such that the difference between the distances is not more than predefined value.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) information processing device; and

(2) computer readable medium storing memory access program.

USE - For accessing memory of an information processing device (claimed) such as integrated circuit (**IC**) **card** e.g. **smart card** and subscriber identification module (SIM) card used in global system for mobile communication(GSM) mobile phone e.g. GSM mobile radio telephone system and in other mobile terminals used for user authentication and electronic commerce.

ADVANTAGE - Since constant hamming distances of data is maintained, **power** consumption caused due to address changes is reduced. Extraction of user information of card is difficult.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of the memory.

pp; 19 DwgNo 6/8

Title Terms: MEMORY; ACCESS; METHOD; MOBILE; TELEPHONE; ACCESS; MEMORY; PORTION; ASSOCIATE; RESPECTIVE; HAMMING; DISTANCE; DIFFER; DISTANCE; MORE ; PREDEFINED; VALUE
Derwent Class: T01; T04; W01
International Patent Class (Main): G06F-001/00; G06F-012/14
File Segment: EPI

19/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013882996 **Image available**
WPI Acc No: 2001-367209/200138
XRPX Acc No: N01-267963

Device, program or system for processing secret information

Patent Assignee: HITACHI LTD (HITA); HITACHI SEISAKUSHO KK (HITA)
Inventor: **FUKUZAWA Y** ; MIYAZAKI K; TAKARAGI K
Number of Countries: 026 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200124439	A1	20010405	WO 99JP5353	A	19990929	200138	B
AU 9959992	A	20010430	AU 9959992	A	19990929	200142	
			WO 99JP5353	A	19990929		
EP 1217783	A1	20020626	EP 99973813	A	19990929	200249	
			WO 99JP5353	A	19990929		
KR 2002025630	A	20020404	WO 99JP5353	A	19990929	200267	
			KR 2000709164	A	20000819		
JP 2001527499	X	20030422	WO 99JP5353	A	19990929	200336	
			JP 2001527499	A	19990929		
KR 373669	B	20030226	WO 99JP5353	A	19990929	200345	
			KR 2000709164	A	20000819		
AU 762650	B	20030703	AU 9959992	A	19990929	200354	
			WO 99JP5353	A	19990929		

Priority Applications (No Type Date): WO 99JP5353 A 19990929
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200124439	A1	J	56	H04L-009/10	
Designated States (National): AU CA CN JP KR SG US					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
AU 9959992	A			H04L-009/10	Based on patent WO 200124439
EP 1217783	A1	E		H04L-009/10	Based on patent WO 200124439
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
KR 2002025630	A			G06F-015/00	
JP 2001527499	X			H04L-009/10	Based on patent WO 200124439
KR 373669	B			G06F-015/00	Previous Publ. patent KR 2002025630 Based on patent WO 200124439
AU 762650	B			H04L-009/10	Previous Publ. patent AU 9959992 Based on patent WO 200124439

Abstract (Basic): WO 200124439 A1

NOVELTY - A secure cryptographic device such as of an **IC card** capable of resisting an attacking method for inferring the internally stored secret information, such as TA (Timing Attack), DPA (Differential **Power** Analysis) or SPA (Simple **Power** Analysis). The internally held secret information is operated in a different manner each time by expressing the secret information and other information used for the operation, thereby making different the operation time, the intensity of radiated electromagnetic wave, and the current consumption.

USE - Device, program or system for processing secret information

DESCRIPTION OF DRAWING(S) - **IC card** (1001)
Operational processing unit (1002)
Data storage unit (1004)
Program storage unit (1005)
Secret key portion information dA (1007)
Secret key portion information dB (1008)
System key (1009)
Expression conversion program (1010)
Elliptical curve cipher decoding program (1011)
Common key cipher decoding program (1012)
Decoding point R (1013)
Enciphered message m (1014)

Decoded message m' (1015)
Input (A)
Output (B)
pp; 56 DwgNo 1/12
Title Terms: DEVICE; PROGRAM; SYSTEM; PROCESS; SECRET; INFORMATION
Derwent Class: T01; T04; W01
International Patent Class (Main): G06F-015/00; H04L-009/10
International Patent Class (Additional): G06F-012/14; G06K-017/00
File Segment: EPI

19/5/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013834529 **Image available**
WPI Acc No: 2001-318741/200134
XRPX Acc No: N01-229079

Data processing apparatus offering high level of security such as computer system particularly microcomputer system

Patent Assignee: HITACHI LTD (HITA); HITACHI ULSI SYSTEMS CO LTD (HISC) ; HITACHI MICON SYSTEM KK (HITA-N)
Inventor: **ENDO T ; FUKUZAWA Y ; KAMINAGA M ; NAGASAKI N ; NAKADA K ; NARIYOSHI Y ; OHKI M ; TAIRA S ; TERAUCHI C ; TSUKAMOTO T ; WATASE H**

Number of Countries: 028 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1073021	A2	20010131	EP 2000113051	A	20000623	200134	B
JP 2001005731	A	20010112	JP 99178750	A	19990624	200134	
KR 2001021026	A	20010315	KR 200034770	A	20000623	200159	
TW 544577	A	20030801	TW 2000111893	A	20000616	200411	

Priority Applications (No Type Date): JP 99178750 A 19990624
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1073021	A2	E	77	G07F-007/10	
	Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI				
JP 2001005731	A		40	G06F-012/14	
KR 2001021026	A			G06F-015/16	
TW 544577	A			G06F-012/14	

Abstract (Basic): EP 1073021 A2

NOVELTY - Apparatus includes at least a first information processing device (0101) connected to a signal line (0113). A device (0114) changes **power** consumption on the signal line during transmission of signal through the signal line in accordance with the actual sate of **power** consumption that would be observed when the device is not used. When a second information-processing device (0102) is connected to the signal line, the data processing apparatus determines a state of second **power** consumption for the state of first **power** consumption on the signal line during signal transmission along the signal line between the information processing devices.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are made for: 1. Information memory device for storing several pieces of information at same storing locations; 2. Data processing apparatus comprising at least an external information memory device, information processor including internal information memory device and a signal line connecting external memory device to information processor and information transfer control device; 3. A card comprising at least two information processing devices connected by a signal line; and 4. An information processing system comprising at least a terminal and a card connectable to one another.

USE - In information processing apparatus, which offers high level of security.

ADVANTAGE - Provides card with high level security, represented by **IC card** or **smart card** . Lowers degree of relationship between data processing in microcomputer chip and its **power** consumption.

DESCRIPTION OF DRAWING(S) - Drawing shows a diagram of basic configuration of first embodiment of data processing apparatus specified in the present application for a patent.

Information processing device (0101, 0102)
Signal line (0113)
Device for changing **power** consumption (0114)
pp; 77 DwgNo 5/40

Title Terms: DATA; PROCESS; APPARATUS; OFFER; HIGH; LEVEL; SECURE; COMPUTER ; SYSTEM; MICROCOMPUTER; SYSTEM
Derwent Class: T01; T04; T05; U21

International Patent Class (Main): G06F-012/14; G06F-015/16; G07F-007/10
International Patent Class (Additional): G06K-019/073
File Segment: EPI

19/5/8 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01458417
Attack-resistant cryptographic method and apparatus
Angriffsresistente kryptographische Verfahren und Vorrichtung
Procede et appareil cryptographique resistant aux attaques
PATENT ASSIGNEE:
Hitachi Ltd., (204155), 6, Kanda Surugandai 4-chome, Chiyoda-ku, Tokyo, (JP), (Applicant designated States: all)
INVENTOR:
Kaminaga, Masahiro, Hitachi, Ltd., Int.Prop.Group , New Marunouchi Bldg. 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Endo, Takashi, Hitachi, Ltd., Int.Prop.Group , New Marunouchi Bldg. 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Watanabe, Takashi, Hitachi, Ltd., Int.Prop.Group, New Marunouchi Bldg. 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP
LEGAL REPRESENTATIVE:
Beetz & Partner Patentanwalte (100712), Steinsdorfstrasse 10, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1248409 A2 021009 (Basic)
EP 1248409 A3 030604
APPLICATION (CC, No, Date): EP 2001130235 011219;
PRIORITY (CC, No, Date): JP 200197964 010330
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/30; G06F-007/72
NOTE:
Figure number on first page: 2
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 021009 A2 Published application without search report
Search Report: 030604 A3 Separate publication of the search report
Examination: 040121 A2 Date of request for examination: 20031121
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200241	795
SPEC A	(English)	200241	7907
Total word count - document A			8702
Total word count - document B			0
Total word count - documents A + B			8702

19/5/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01452325
Tamper resistant device
Betrugssichere Vorrichtung
Dispositif resistant a la fraude
PATENT ASSIGNEE:
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
INVENTOR:
Endo, Takashi, Hitachi, Ltd., Int. Prop. Gp. , New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Kaminaga, Masahiro, Hitachi, Ltd., Int. Prop. Gp. , New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Watanabe, Takashi, Hitachi, Ltd., Int. Prop. Gp., New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Ohki, Masaru, Hitachi, Ltd., Int. Prop. Gp. , New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP
LEGAL REPRESENTATIVE:
Beetz & Partner Patentanwalte (100712), Steinsdorfstrasse 10, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1244077 A2 020925 (Basic)
APPLICATION (CC, No, Date): EP 2001120625 010829;
PRIORITY (CC, No, Date): JP 200146250 010222
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G07F-007/10; G06K-019/073

ABSTRACT EP 1244077 A2
It is an object of the disclosed technology to provide a tamper resistance device such as a card member having high security. The disclosed technology provides a solution to problems by reduction of the degree of relationship between information processed in the card member such as a chip for an **IC card** and current consumption for the processing.
As a means for solving the problem, there is provided a method for reducing the degree of relationship between the magnitude of a current consumed by the chip for an **IC card** and information processed by the chip. In accordance with this method, information is transformed by using data for disturbance of the information prior to processing and, after the processing of the transformed data, the processed transformed information is subjected to inverse transformation using the data for disturbance of the information to result in correct processed information. The method is characterized in that the hamming weight of the data for disturbance of information is all but constant.
ABSTRACT WORD COUNT: 167
NOTE:
Figure number on first page: 13

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020925 A2 Published application without search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 200239 2346
SPEC A (English) 200239 20776
Total word count - document A 23122
Total word count - document B 0
Total word count - documents A + B 23122

19/5/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01447133
Tamper-resistant processing method
Betrugssicheres Verarbeitungsverfahren
Methode de traitement inviolable
PATENT ASSIGNEE:
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
INVENTOR:
Kaminaga, Masahiro, Hitachi, Ltd., Int. Prop. Gp. , New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Endo, Takashi, Hitachi, Ltd., Int. Prop. Gp. , New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Watanabe, Takashi, Hitachi, Ltd., Int. Prop. Gp., New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Ohki, Masaru, Hitachi, Ltd., Int. Prop. Gp. , New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP
LEGAL REPRESENTATIVE:
Beetz & Partner Patentanwalte (100712), Steinsdorfstrasse 10, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1239365 A2 020911 (Basic)
APPLICATION (CC, No, Date): EP 2001119739 010827;
PRIORITY (CC, No, Date): JP 200161544 010306
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G06F-007/72

ABSTRACT EP 1239365 A2
The subject of the disclosed technology is, when a crypto-processing is performed utilizing an information processing device buried in an **IC card** , etc., to decrease the relationship between the waveform of the consumption current and the contents of the crypto-processing as a countermeasure against a tamper which observes the waveform of a consumption current.
A solution means is shown in the following. When a decryption processing of an RSA cryptogram is performed according to CRT, in step 608, for every unit bit block of XP a modular exponentiation calculation is performed, and the partial result of CP up to the calculated bit block is stored in a memory. In step 609, for every unit bit block of XQ a modular exponentiation calculation is performed and the partial result of CQ up to the calculated bit block is stored in a memory. In step 606, a random number is generated, and in step 607, it is decided that step 608 is to be executed or step 609 is to be executed corresponding to the value of the random number.
ABSTRACT WORD COUNT: 179
NOTE:
Figure number on first page: 6

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020911 A2 Published application without search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200237	908
SPEC A	(English)	200237	12099
Total word count - document A			13007
Total word count - document B			0
Total word count - documents A + B			13007

19/5/12 (Item 12 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01446148

Fault detection method for cryptographic process
Verfahren zur Fehlererkennung bei einem kryptographischen Vorgang
Procede de detection d'erreur se produisant lors d' une operation cryptographique

PATENT ASSIGNEE:
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
INVENTOR:
Kaminaga, Masahiro, New Marunouchi Bldg. , Hitachi Ltd., Intell.Prop. Group, 5-1-1 Marunouchi, Chiyoda-ku, Tokyo 100-8220, (JP)
Endo, Takashi, New Marunouchi Bldg. , Hitachi Ltd., Intell.Prop. Group, 5-1-1 Marunouchi, Chiyoda-ku, Tokyo 100-8220, (JP)
Watanabe, Takashi, New Marunouchi Bldg., Hitachi Ltd., Intell.Prop. Group, 5-1-1 Marunouchi, Chiyoda-ku, Tokyo 100-8220, (JP)
Ohki, Masaru, New Marunouchi Bldg. , Oitachi Ltd., Intell.Prop. Group, 5-1-1 Marunouchi, Chiyoda-ku, Tokyo 100-8220, (JP
LEGAL REPRESENTATIVE:
Beetz & Partner Patentanwalte (100712), Steinsdorfstrasse 10, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1237322 A2 020904 (Basic)
EP 1237322 A3 030813
APPLICATION (CC, No, Date): EP 2001119671 010822;
PRIORITY (CC, No, Date): JP 200158087 010302
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/06; H04L-009/30

ABSTRACT EP 1237322 A2
The disclosed techniques are as shown below. The subject of the invention is to provide a crypto-processing method capable to confront an attack, which intentionally causes an erroneous operation and takes out secret information to be done against a device which performs a crypto-processing inside the device such as an **IC card** .
The solution means for such an attack is shown below. A ciphertext C is received through the I/O port on an **IC card** , etc. (step 601), the ciphertext C is stored on a RAM (step 602), a decryption process of the ciphertext C is performed (step 603), and the processing result Z is stored on a RAM (step 604). For the processing result Z, an encryption process is executed (step 605), and the processing result W and the original plaintext C are compared with each other (step 606). When the processing result W coincides with the original plaintext C, the plaintext Z is output to the I/O port (step 608), and if not, a reset is effected (step 607).
ABSTRACT WORD COUNT: 172
NOTE:
Figure number on first page: 6

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020904 A2 Published application without search report
Search Report: 030813 A3 Separate publication of the search report
Examination: 040204 A2 Date of request for examination: 20031208
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 200236 531
SPEC A (English) 200236 6806
Total word count - document A 7337
Total word count - document B 0
Total word count - documents A + B 7337

19/5/15 (Item 15 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01405247
IC card **system and** IC card
IC-Kartensystem und IC-Karte
Systeme de carte a puce et carte a puce
PATENT ASSIGNEE:
Hitachi, Ltd., (204151), 6, Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
INVENTOR:
Sato, Akiko, Hitachi, Ltd., Intell. Property Group, New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Mishina, Yusuke, Hitachi, Ltd. Intell. Prop. Group, New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Ohki, Masaru, Hitachi, Ltd. Intell. Property Group , New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Baba, Satomi, Hitachi, Ltd. Intell. Property Group, New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP)
Matsui, Yutaka, Hitachi, Ltd. Intell. Prop. Group, New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8220, (JP
LEGAL REPRESENTATIVE:
Strehl Schubel-Hopf & Partner (100941), Maximilianstrasse 54, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1189157 A2 020320 (Basic)
EP 1189157 A3 030917
APPLICATION (CC, No, Date): EP 2000117662 000816;
PRIORITY (CC, No, Date): JP 2000249182 000811
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G07F-007/10; G06F-017/60; G06K-019/073

ABSTRACT EP 1189157 A2
The present invention provides an **IC card** that allows a service provider doing a business of loading an application into the **IC card** to dynamically load the application into the **IC card** safely after the issuance of the **IC card** without making a contract directly with a card issuer issuing the **IC card** and without establishing a communication with the card issuer. The present invention also provides an **IC - card** issuing method for issuing the **IC card** and an **IC - card** operating method using the **IC card** .The card issuer issuing the **IC card** hands over an encryption key in advance to a third party other than the card issuer in order to entrust the third party with work to authenticate an application to be loaded or to allow the third party to function as an agent on behalf of the card issuer. The card issuer issues an agent certification to the third party to be used as evidence showing that the third party is an agent representing the card issuer. A program having a function to verify validity of the agent certification into the **IC card** is capable of verifying validity of an application to be loaded.
ABSTRACT WORD COUNT: 196
NOTE:
Figure number on first page: 6

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020320 A2 Published application without search report
Change: 030917 A2 International Patent Classification changed: 20030731
Search Report: 030917 A3 Separate publication of the search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 200212 2555
SPEC A (English) 200212 15259
Total word count - document A 17814

19/5/31 (Item 31 from file: 347)
DIALOG(R)File 347:JAPIO

06673973 **Image available**
IC CARD AND SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE

PUB. NO.: 2000-259799 [JP 2000259799 A]
PUBLISHED: September 22, 2000 (20000922)
INVENTOR(s): **WATASE HIROSHI**
NAGASAKI NOBUTAKA
TSUKAMOTO TAKU
TAIRA SATOSHI
TAKAHASHI MASAAKI
NAKADA KUNIHIKO
TERAUCHI CHIAKI
OKI MASARU
KAMINAGA MASAHIRO
APPLICANT(s): HITACHI LTD
HITACHI ULSI SYSTEMS CO LTD
APPL. NO.: 11-061561 [JP 9961561]
FILED: March 09, 1999 (19990309)
INTL CLASS: G06K-019/07; G06F-012/14; G06F-015/78; H01L-027/10

ABSTRACT

PROBLEM TO BE SOLVED: To provide an **IC card** and a semiconductor integrated circuit device realizing the enhancement of security.

SOLUTION: In the **IC card** or semiconductor integrated circuit device which includes a data processor and a ROM where data processing procedures including security information processing by such a data processor are written and to which an operation **voltage** is applied by such a manner that an external terminal is electrically connected to an external device such as a reader-writer and in which a data processing operation following the data processing procedures is performed, the security is obtained by making it substantially impossible to perform data dependence analysis such as to compare a current waveform on the time base because the procedure and timing for cipher processing change every time and a consumption current waveform in the case of being seen from a time base change by providing a means that makes the timing of the data processing procedures change.

19/5/32 **(Item 32 from file: 347)**
DIALOG(R)File 347:JAPIO

06673958 **Image available**
IC CARD AND SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE

PUB. NO.: 2000-259784 [JP 2000259784 A]
PUBLISHED: September 22, 2000 (20000922)
INVENTOR(s): **NARIYOSHI YUICHIRO**
NAGASAKI NOBUTAKA
TSUKAMOTO TAKU
KANAI TAKEO
MIZUNO HIROTAKA
NAKADA KUNIHIKO
TERAUCHI CHIAKI
OKI MASARU
KAMINAGA MASAHIRO
APPLICANT(s): HITACHI LTD
HITACHI ULSI SYSTEMS CO LTD
APPL. NO.: 11-061551 [JP 9961551]
FILED: March 09, 1999 (19990309)
INTL CLASS: G06K-017/00; G06F-012/14

ABSTRACT

PROBLEM TO BE SOLVED: To provide an **IC card** and a semiconductor integrated circuit device, whose security is strengthened.

SOLUTION: In the integrated circuit device which includes the **IC card** or a data processor to which operation **voltage** is supplied by electrically connecting an external terminal and a reader/writer and in which the input/ output operation of data is executed and a ROM in which a data processing procedure by the data processor is written and in which the input/output operation of data is executed according to the data processing procedure, a false current generation circuit 210 generating current made to be an irregular current value regardless of an inner circuit operation accompanying the input/tout operation of data between the reader/writer and the external device and making current flow to a **power** terminal to which operation **voltage** is supplied is installed.

```
Set     Items   Description
S1      13725   SMARTCARD? OR CHIPCARD? OR ICCARD? OR MONDEX? OR PHYSICAL(-
             )TOKEN? OR (SMART OR CHIP OR IC)()CARD? ?
S2    6177019   POWER? OR VOLTAGE? OR AMP OR AMPS OR AMPERE? OR WATT? ? OR
             CURRENT?
S3     518256   S2(2N)(CONTROL? OR FLUCTUAT? OR CHANG? OR VARY OR VARIES OR
              CHANG? OR MODERATE OR MEASUR? OR MONITOR?)
S4       3825   S1(15N)(ENCRYPT? OR CRYPTO? OR SECUR? OR SAFE? OR DES OR R-
             SA OR PROTECT? OR ENCIPHER? OR ENCYPHER? OR SPA OR TA OR ATTA-
             CK? OR DPA)
S5         43   S3 AND S4
S6        115   S3 AND S1
S7         28   S6 AND (LINE? OR BUS OR BUSSES OR PATH OR PATHS OR ROUTE OR
              ROUTES OR WIRE OR WIRES)
S8         60   S7 OR S5
S9         38   RD (unique items)
S10        20   S9 NOT PY>1999
S11        20   S10 NOT PD=19990624:20010624
S12        20   S11 NOT PD=20010624:20040501
S13        53   S1(5N)(SPA OR TA OR DPA OR SIMPLE()POWER()ANALYSIS OR DIFF-
             ERENTIAL()POWER()ANALYSIS OR TIMING()ATTACK?)
S14        72   S12 OR S13
S15        51   RD (unique items)
S16        21   S15 NOT PY>1999
File   8:Ei Compendex(R) 1970-2004/Apr W3
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/Apr
         (c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/Feb 27
         (c) 2004 EBSCO Publishing
File  65:Inside Conferences 1993-2004/Apr W4
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Apr W3
         (c) 2004 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2004/Apr W2
         (c)2004 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2004/Apr 30
         (c) 2004 The Gale Group
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File   6:NTIS 1964-2004/May W1
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2004/Apr W3
         (c) 2004 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Apr W4
         (c) 2004 Inst for Sci Info
File  62:SPIN(R) 1975-2004/Mar W1
         (c) 2004 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Mar
         (c) 2004 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2004/Apr W2
         (c) 2004 FIZ TECHNIK
```

16/5/9 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6650550 INSPEC Abstract Number: B2000-08-6120D-043, C2000-08-1260C-026
Title: Resistance against differential power analysis for elliptic curve cryptosystems
Author(s): Coron, J.-S.
Author Affiliation: Ecole Normale Superieure, Paris, France
Conference Title: Cryptographic Hardware and Embedded Systems. First International Workshop, CHES'99. Proceedings (Lecture Notes in Computer Science Volume 1717) p.292-302
Editor(s): Koc, C.K.; Paar, C.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1999 Country of Publication: Germany 352 pp.
ISBN: 3 540 66646 X Material Identity Number: XX-1999-03503
Conference Title: Cryptographic Hardware and Embedded Systems. First International Workshop, CHES'99
Conference Date: 12-13 Aug. 1999 Conference Location: Worcester, MA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Theoretical (T)
Abstract: Differential power analysis, first introduced by Kocher et al. (1998), is a powerful technique allowing us to recover secret smart card information by **monitoring power** signals. In Kocher et al., a specific **DPA attack** against **smart cards** running the **DES** algorithm was described. As few as 1000 **encryptions** were sufficient to recover the secret key. We generalize the DPA attack to elliptic curve (EC) cryptosystems and describe a DPA on EC Diffie-Hellman key exchange and EC El-Gamal type **encryption** . Those **attacks** enable us to recover the private key stored inside the **smart card** . Moreover, we suggest countermeasures that thwart our **attack** . (18 Refs)
Subfile: B C
Descriptors: cryptography; monitoring; power consumption; smart cards
Identifiers: differential power analysis; elliptic curve cryptosystems; smart card information; **power** signal **monitoring** ; secret key; Diffie-Hellman key exchange; El-Gamal type encryption; countermeasures
Class Codes: B6120D (Cryptography); C1260C (Cryptography theory); C6130S (Data security)

16/5/10 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6451396 INSPEC Abstract Number: C2000-02-6130S-038
Title: Investigations of power analysis attacks **on** smart cards
Author(s): Messerges, T.S.; Dabbish, E.A.; Sloan, R.H.
Author Affiliation: Motorola, USA
Conference Title: Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99) p.151-61
Publisher: USENIX Assoc, Berkeley, CA, USA
Publication Date: 1999 Country of Publication: USA 185 pp.
ISBN: 1 880446 34 0 Material Identity Number: XX-1999-02277
Conference Title: Proceedings of the USENIX Workshop on Smartcard Technology
Conference Date: 10-11 May 1999 Conference Location: Chicago, IL, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: This paper presents actual results from **monitoring** smart card **power** signals and introduces techniques that help maximize such side-channel information. Adversaries will obviously choose attacks that maximize side-channel information, so it is very important that the strongest attacks be considered when designing defensive strategies. In this paper, power analysis techniques used to attack DES are reviewed and analyzed. The noise characteristics of the power signals are examined and an approach to model the signal to noise ratio is proposed. Test results from **monitoring power** signals are provided. Next, approaches to maximize the information content of the power signals are developed and tested. These results provide guidance for designing **smart card** solutions that are **secure** against power analysis **attacks** . (16 Refs)
Subfile: C
Descriptors: security of data; smart cards
Identifiers: power analysis attacks; smart card **power** signal **monitoring** ; side-channel information; defensive strategies; noise characteristics; signal to noise ratio modelling; information content; security
Class Codes: C6130S (Data security)

```
Set     Items   Description
S1     134965   SMARTCARD? OR CHIPCARD? OR ICCARD? OR MONDEX? OR PHYSICAL(-
             )TOKEN? OR (SMART OR CHIP OR IC)()CARD? ?
S2   14723757   POWER? OR VOLTAGE? OR AMP OR AMPS OR AMPERE? OR WATT? ? OR
             CURRENT?
S3     423515   S2(2N)(CONTROL? OR FLUCTUAT? OR CHANG? OR VARY OR VARIES OR
              CHANG? OR MODERATE OR MEASUR? OR MONITOR?)
S4      44834   S1(15N)(ENCRYPT? OR CRYPTO? OR SECUR? OR SAFE? OR DES OR R-
             SA OR PROTECT? OR ENCIPHER? OR ENCYPHER? OR SPA OR TA OR ATTA-
             CK? OR DPA)
S5        145   S3 (S) S4
S6        319   S3 (S) S1
S7         59   S6 (S) (LINE? OR BUS OR BUSSES OR PATH OR PATHS OR ROUTE OR
              ROUTES OR WIRE OR WIRES)
S8        114   S1(5N)(SPA OR TA OR DPA OR SIMPLE()POWER()ANALYSIS OR DIFF-
             ERENTIAL()POWER()ANALYSIS OR TIMING()ATTACK?)
S9         74   S3(5N)S4
S10       121   S9 OR S7
S11        59   RD (unique items)
S12        28   S11 NOT PY>1999
S13        26   S12 NOT PD=19990624:20010624
S14        26   S13 NOT PD=20010624:20040501
File 275:Gale Group Computer DB(TM) 1983-2004/Apr 30
         (c) 2004 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2004/Apr 30
         (c) 2004 The Gale group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Apr 30
         (c) 2004 The Gale Group
File  16:Gale Group PROMT(R) 1990-2004/Apr 30
         (c) 2004 The Gale Group
File 624:McGraw-Hill Publications 1985-2004/Apr 29
         (c) 2004 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2004/Apr W4
         (c) 2004 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 141:Readers Guide 1983-2004/Apr
         (c) 2004 The HW Wilson Co
File 239:Mathsci 1940-2004/Jun
         (c) 2004 American Mathematical Society
File 696:DIALOG Telecom. Newsletters 1995-2004/Apr 29
         (c) 2004 The Dialog Corp.
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Apr 29
         (c) 2004 The Gale Group
File 674:Computer News Fulltext 1989-2004/Apr W3
         (c) 2004 IDG Communications
File  88:Gale Group Business A.R.T.S. 1976-2004/Apr 29
         (c) 2004 The Gale Group
File 369:New Scientist 1994-2004/Apr W4
         (c) 2004 Reed Business Information Ltd.
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2004/Apr 30
         (c) 2004 ProQuest Info&Learning
File  15:ABI/Inform(R) 1971-2004/Apr 30
         (c) 2004 ProQuest Info&Learning
File   9:Business & Industry(R) Jul/1994-2004/Apr 29
         (c) 2004  The Gale Group
File  13:BAMP 2004/Apr W2
         (c) 2004  The Gale Group
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 647:CMP  Computer Fulltext 1988-2004/Apr W3
         (c) 2004 CMP Media, LLC
File  98:General Sci Abs/Full-Text 1984-2004/Apr
         (c) 2004 The HW Wilson Co.
File 148:Gale Group Trade & Industry DB 1976-2004/Apr 30
         (c)2004 The Gale Group
```

File 634:San Jose Mercury Jun 1985-2004/Apr 29

14/3,K/5 (Item 1 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)

05293029 SUPPLIER NUMBER: 53534831 (USE FORMAT 7 OR 9 FOR FULL TEXT)
SCIENCE NEWS of the Year. (recap of science news from 1998)
Miller, Julie Ann
Science News, 402(1)
Dec 19, 1998
ISSN: 0036-8423 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 5390 LINE COUNT: 00445

... cubic packing--fills space more efficiently than any other arrangement of identical spheres (154: 103*).

* **Cryptographers** showed that **monitoring** the **power** usage of a **smart card** 's microcircuitry can provide data for breaching the card's **security** (153: 388*). They also dramatically reduced the time required to identify the numerical key for...

14/3,K/6 (Item 2 from file: 47)

05195059 SUPPLIER NUMBER: 20912201 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Power cracking of cash card codes.(Science News of the Week)
Peterson, Ivars
Science News, v153, n25, p388(1)
June 20, 1998
ISSN: 0036-8423 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 585 LINE COUNT: 00052

That microcircuitry also makes it vulnerable to **attack** . **Cryptographers** have now identified techniques for breaking the **security** system built into a **smart card** . They cracked the codes by **monitoring power** consumption as the circuitry performed its cryptographic operations.

"We have implemented these attacks against a...

...or exploited processing errors (SN: 2/1/97, p. 78).

In the new threat, an **attacker** can use less expensive equipment to monitor a **smart card** 's electronic responses. **Fluctuations** in **power** consumption correspond to different stages in a **cryptographic** process. By magnifying the signal, it is possible to detect individual microprocessor instructions and distinguish...

14/3,K/10 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07356999 Supplier Number: 58916703 (USE FORMAT 7 FOR FULLTEXT)
DIGITAL PATROL.
Marlin, Steven
Bank Systems + Technology, v35, n10, p40
Oct, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2454

... at The Tower Group, Newton, Mass.
The West Coast cryptographers, led by Paul Kocher of **Cryptography** Research, a San Francisco consulting firm, obtained the secret **encryption** keys from a **smart card** through a technique called differential power analysis (**DPA**), in which an oscilloscope **measures** the electrical **power** consumed during a **smart card** 's operations. The power consumption information is statistically analyzed to get information about what the...

14/3,K/12 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06000107 Supplier Number: 53383321 (USE FORMAT 7 FOR FULLTEXT)
Attacking the Smart Card Fortress.
Demery, Paul
Credit Card Management, v11, n6, p26(1)
Sept, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2788

... of altering chip circuitry to mask the power consumption, and modifying a chip's algorithm **encryption** software to make it more difficult to determine a key by **monitoring power** use.
Bull **Smart Cards** & Terminals, a leading supplier with more than 100 million

14/3,K/22 (Item 2 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

2259020 Supplier Number: 02259020 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Attacking the Smart Card Fortress
(High-tech research has been able to break smartcard security features, but some question the reality of the threat)
Credit Card Management, v 11, n 6, p 26+
September 1998
DOCUMENT TYPE: Journal ISSN: 0896-9329 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2350

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...of altering chip circuitry to mask the power consumption, and modifying a chip's algorithm **encryption** software to make it more difficult to determine a key by **monitoring power** use.

Bull **Smart Cards** & Terminals, a leading supplier with more than 100 million smart cards deployed in Europe, says...

```
Set     Items   Description
S1      15966   SMARTCARD? OR CHIPCARD? OR ICCARD? OR MONDEX? OR PHYSICAL(-
             )TOKEN? OR (SMART OR CHIP OR IC)()CARD? ?
S2     808319   POWER? OR VOLTAGE? OR AMP OR AMPS OR AMPERE? OR WATT? ? OR
             CURRENT?
S3     159413   S2(2N)(CONTROL? OR FLUCTUAT? OR CHANG? OR VARY OR VARIES OR
              CHANG? OR MODERATE OR MEASUR? OR MONITOR?)
S4       4534   S1(15N)(ENCRYPT? OR CRYPTO? OR SECUR? OR SAFE? OR DES OR R-
             SA OR PROTECT? OR ENCIPHER? OR ENCYPHER? OR SPA OR TA OR ATTA-
             CK? OR DPA)
S5         33   S3(10N)S4
S6          9   S5 AND IC=(G06F-012? OR G06F-015? OR G06F-007?)
S7         94   S3(S)S4
S8         15   S7 AND IC=(G06F-012? OR G06F-015? OR G06F-007?)
S9         15   S8 OR S6
S10        15   IDPAT (sorted in duplicate/non-duplicate order)
S11        15   IDPAT (primary/non-duplicate records only)
S12        56   S7 AND IC=(G06F? OR H04L? OR H04K?)
S13        41   S12 NOT S8
S14        24   S13 NOT PD=19990624:20010624
S15         5   S14 NOT PD=20010624:20040501
File 348:EUROPEAN PATENTS 1978-2004/Apr W04
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040415,UT=20040408
         (c) 2004 WIPO/Univentio
```

```
Set     Items   Description
S1      15966   SMARTCARD? OR CHIPCARD? OR ICCARD? OR MONDEX? OR PHYSICAL(-
             )TOKEN? OR (SMART OR CHIP OR IC)()CARD? ?
S2     808319   POWER? OR VOLTAGE? OR AMP OR AMPS OR AMPERE? OR WATT? ? OR
             CURRENT?
S3     159413   S2(2N)(CONTROL? OR FLUCTUAT? OR CHANG? OR VARY OR VARIES OR
              CHANG? OR MODERATE OR MEASUR? OR MONITOR?)
S4       4534   S1(15N)(ENCRYPT? OR CRYPTO? OR SECUR? OR SAFE? OR DES OR R-
             SA OR PROTECT? OR ENCIPHER? OR ENCYPHER? OR SPA OR TA OR ATTA-
             CK? OR DPA)
S5         33   S3(10N)S4
S6          9   S5 AND IC=(G06F-012? OR G06F-015? OR G06F-007?)
S7         94   S3(S)S4
S8         15   S7 AND IC=(G06F-012? OR G06F-015? OR G06F-007?)
S9         15   S8 OR S6
S10        15   IDPAT (sorted in duplicate/non-duplicate order)
S11        15   IDPAT (primary/non-duplicate records only)
File 348:EUROPEAN PATENTS 1978-2004/Apr W04
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040415,UT=20040408
         (c) 2004 WIPO/Univentio
```

11/3,K/14 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00579138 **Image available**
METHOD AND APPARATUS FOR MINIMIZING DIFFERENTIAL POWER ATTACKS ON PROCESSORS
PROCEDE ET APPAREIL PERMETTANT DE MINIMISER DES ATTAQUES MASSIVES DE TYPE DIFFERENTIEL SUR DES PROCESSEURS
Patent Applicant/Assignee:
CERTICOM CORP,
PEZESHKI Farhad,
LAMBERT Robert J,
Inventor(s):
PEZESHKI Farhad,
LAMBERT Robert J,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200042511 A1 20000720 (WO 0042511)
Application: WO 2000CA21 20000111 (PCT/WO CA0000021)
Priority Application: CA 2258338 19990111
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 4815

Main International Patent Class: **G06F-012/14**
Fulltext Availability:
Detailed Description

Detailed Description
... analyzed to find the entire secret key, compromising the system.

In the simple power analysis (**SPA**) **attacks** on **smart cards** and other **secure** tokens, an **attacker** directly measures the token's **power** consumption **changes** over time. The amount of **power** consumed **varies** depending on the executed microprocessor instructions.

A large calculation such as elliptic curve (EC) additions...

...to expose logic gates, microprocessor operation and ultimately the software implementations.

In software implementation of **cryptographic** routines, particularly on **smart cards** , branches in program flow are particularly vulnerable to **power** analysis **measurements** .

Generally, where the program flow reaches a branch, then based on some distinguishing value V...

11/3,K/15 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00298087 **Image available**
SECURE COMPUTER MEMORY CARD
CARTE MEMOIRE DE SECURITE POUR ORDINATEUR
Patent Applicant/Assignee:
TELEQUIP CORPORATION,
Inventor(s):
JONES Michael F,
ZACHAI Arthur,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9516238 A1 19950615

Application: WO 94US13898 19941205 (PCT/WO US9413898)
Priority Application: US 93161854 19931206
Designated States: AM AT AU BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW NL NO NZ PL PT RO RU SD SE SI SK TJ TT UA UZ VN KE MW SD SZ AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 5925

Main International Patent Class: **G06F-012/14**
Fulltext Availability:
Detailed Description

Detailed Description
... card and (2)
knowledge of the memory card access password stored in the card's **secure**

substorage unit.

The **smartcard** integrated circuit advantageously stores such passwords, public key and secret key values, and/or digital...

...via the serial interface, but thereafter prevents that password value from being accessed. For enhanced **security** , the
smartcard integrated circuit includes means for **monitoring** **voltages** and
frequencies to detect abnormal conditions which may indicate an attempt to tamper with the...

```
Set     Items   Description
S1      30973   SMARTCARD? OR CHIPCARD? OR ICCARD? OR MONDEX? OR PHYSICAL(-
             )TOKEN? OR (SMART OR CHIP OR IC)()CARD? ?
S2    2900693   POWER? OR VOLTAGE? OR AMP OR AMPS OR AMPERE? OR WATT? ? OR
             CURRENT?
S3     384258   S2(2N)(CONTROL? OR FLUCTUAT? OR CHANG? OR VARY OR VARIES OR
              MODERATE OR MEASUR? OR MONITOR?)
S4    2001956   ENCRYPT? OR CRYPTO? OR SECUR? OR SAFE? OR DES OR RSA OR KE-
             Y? ? OR PROTECT? OR ENCIPHER? OR ENCYPHER? OR ATTACK? OR SPA -
             OR TA OR DPA
S5        130   S1 AND S3 AND S4
S6         17   S5 AND IC=(G06F-015/16 OR G06F-012/14 OR G06F-007/10)
S7         52   S5 AND MC=(T01-D01 OR T01-F05B3 OR T01-H01B3A OR T01-H01C2
             OR T01-J12C OR T04-K02 OR T05-H02C5C OR U21-C02)
S8       4005   S1(10N)(S3 OR S4)
S9         34   S7 AND S8
S10        41   S6 OR S9
S11        41   IDPAT (sorted in duplicate/non-duplicate order)
S12        41   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2003/Dec(Updated 040402)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200427
         (c) 2004  Thomson Derwent
```

12/5/4 **(Item 4 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

015562796 **Image available**
WPI Acc No: 2003-624952/200359
XRPX Acc No: N03-497206
Integrated circuit chip protection **method e.g. for** current fluctuation protection **, involves using random number generator with linear feedback shift register for emitting electromagnetic noise and reducing signal-to-noise ratio**
Patent Assignee: SILVERBROOK RES PTY LTD (SILV-N)
Inventor: SILVERBROOK K; WALMSLEY S R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6566858	B1	20030520	US 98112763	A	19980710	200359	B

Priority Applications (No Type Date): US 98112763 A 19980710
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6566858	B1		4	G01R-035/00	

Abstract (Basic): US 6566858 B1
NOVELTY - The method involves using a random number generator including a linear feedback shift register (LFSR) for emitting electromagnetic noise and reducing the signal-to-noise ratio to obscure the information in the current signal flowing through the integrated circuit (IC).
USE - For **protecting** tamper proof integrated circuit (IC) chip (claimed) from **current fluctuations , smart cards ,** authentication chips, electronic **keys** and **cryptographic** equipment. Also used as source of pseudo-random bits for other tamper prevention and detection circuit. Also for use in Artcam device.
ADVANTAGE - The noise generator causes enough state changes in each cycle to obscure any meaningful information in the current signal. The clock used for noise generator is supplied at maximum clock rate for chip to generate as much noise as possible.
DESCRIPTION OF DRAWING(S) - The figure depicts an explanatory view of linear feedback shift register having 64-bit maximal period.
pp; 4 DwgNo 1/1
Title Terms: INTEGRATE; CIRCUIT; CHIP; **PROTECT** ; METHOD; CURRENT; FLUCTUATION; **PROTECT** ; RANDOM; NUMBER; GENERATOR; LINEAR; FEEDBACK; SHIFT; REGISTER; EMIT; ELECTROMAGNET; NOISE; REDUCE; SIGNAL; NOISE; RATIO
Derwent Class: T01; U11; U13; U23; U24
International Patent Class (Main): G01R-035/00
File Segment: EPI

12/5/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014739455
WPI Acc No: 2002-560160/200260
XRPX Acc No: N02-443488
Method for protecting **electronic component executing** cryptographic **algorithm against** current measurement attack , **comprises factorization of exponential in algorithm and permutation of the factors**
Patent Assignee: GEMPLUS SCA (GEMP-N)
Inventor: AMIEL F; NACCACHE D
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2818846	A1	20020628	FR 200016993	A	20001222	200260	B

Priority Applications (No Type Date): FR 200016993 A 20001222
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2818846	A1		25	H04L-009/28	

Abstract (Basic): FR 2818846 A1
NOVELTY - Electronic components which execute **cryptographic** algorithms involving exponentials may be **protected** against **current measurement** types of **attack** by replacing the exponent (x) with factors (x1,x2,x3,xi) giving the same product, and then using a random permutation for the order in which the factors are processed during each calculation stage
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are made for a **smart card** which uses the **protective** method
USE - To **protect** electronic components processing **cryptographic** algorithms against **current measurement attack**
ADVANTAGE - The method varies the factor order for algorithm exponentials from one calculation stage to another making **current measurement attack** impractical
pp; 25 DwgNo 0/0
Title Terms: METHOD; **PROTECT** ; ELECTRONIC; COMPONENT; EXECUTE; **CRYPTOGRAPHIC** ; ALGORITHM; CURRENT; MEASURE; **ATTACK** ; COMPRISE; EXPONENTIAL; ALGORITHM; PERMUTATION; FACTOR
Derwent Class: T01; T04; W01
International Patent Class (Main): H04L-009/28
International Patent Class (Additional): G06K-019/07; H04K-003/00
File Segment: EPI

12/5/26 **(Item 26 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

013043571 **Image available**
WPI Acc No: 2000-215424/200019
Related WPI Acc No: 2001-143544
XRPX Acc No: N00-162192

Portable non-contact IC card **reader has control unit that supplies power to reading mechanism and another control unit, only during accessing of non-contact** IC card

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 2000040133	A	20000208	JP 98222300	A	19980722	200019 B

Priority Applications (No Type Date): JP 98222300 A 19980722
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000040133	A		18	G06K-017/00	

Abstract (Basic): JP 2000040133 A

NOVELTY - A control unit (10) controls one of reading mechanism (11) that reads out instructions from non-contact **IC card** (C), based on reception of user demand information from information transmitter via information selector. Another control unit (6) supplies power to reading mechanism and control unit (10), only during accessing of non-contact **IC card** . DETAILED DESCRIPTION - Irreversible degradation of charging unit (5) by overcharge and overdischarge of charging current and charging voltage, is prevented by **protection** unit.

USE - Portable non-contact **IC card** reader.

ADVANTAGE - Since the electric **power control** unit supplies **power** to reading mechanism and another control unit only during **IC card** accessing, power consumption is reduced. DESCRIPTION OF DRAWING(S) - The figure shows block diagram of non-contact **IC card** reader. (5) Charging unit; (6,10) Control units; (11) Reading mechanism; (C) Non-contact **IC card** .

Dwg.1/17

Title Terms: PORTABLE; NON; CONTACT; IC; CARD; READ; CONTROL; UNIT; SUPPLY; POWER; READ; MECHANISM; CONTROL; UNIT; ACCESS; NON; CONTACT; IC; CARD
Derwent Class: T04
International Patent Class (Main): G06K-017/00
File Segment: EPI

12/5/27 **(Item 27 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

012945157 **Image available**
WPI Acc No: 2000-117010/200010
XRPX Acc No: N00-088576
Computational method of using secret key **to** encrypt **message, balanced for leak minimization, e.g. in** smart cards **and other** cryptographic **systems**
Patent Assignee: CRYPTOGRAPHY RES INC (CRYP-N); JAFFE J M (JAFF-I); JUN B C (JUNB-I); KOCHER P C (KOCH-I)
Inventor: JAFFE J M; JUN B C; KOCHER P C
Number of Countries: 083 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9967766	A2	19991229	WO 99US12739	A	19990603	200010 B
AU 9962384	A	20000110	AU 9962384	A	19990603	200025
EP 1088295	A2	20010404	EP 99949533	A	19990603	200120
			WO 99US12739	A	19990603	
US 6510518	B1	20030121	US 9887879	P	19980603	200309
			US 99325611	A	19990603	
US 20030140240	A1	20030724	US 9887879	P	19980603	200352
			US 99325611	A	19990603	
			US 2003346848	A	20030117	
US 6654884	B2	20031125	US 9887879	P	19980603	200378
			US 99325611	A	19990603	
			US 2003346848	A	20030117	

Priority Applications (No Type Date): US 9887879 P 19980603; US 99325611 A 19990603; US 2003346848 A 20030117
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9967766	A2	E	39	G09C-001/12	
Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW					
AU 9962384	A			G09C-001/12	Based on patent WO 9967766
EP 1088295	A2	E		G09C-001/12	Based on patent WO 9967766
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
US 6510518	B1			G06F-001/24	Provisional application US 9887879
US 20030140240	A1			G06F-011/30	Provisional application US 9887879 Cont of application US 99325611 Cont of patent US 6510518
US 6654884	B2			G06F-001/24	Provisional application US 9887879 Cont of application US 99325611 Cont of patent US 6510518

Abstract (Basic): WO 9967766 A2

NOVELTY - The representation of data, the number of state transitions at each computational step and the Hamming weights of all operands are independent of computation inputs, intermediate values or results.

DETAILED DESCRIPTION - The method involves receiving a message for **cryptographical** processing. A hardware device performs a number of **cryptographical** suboperations on the message. Each suboperation involves taking an input to an output, via at least one intermediate, including a number of computational state transformations, where the number of transformations does not depend on the massage or the **key** . The Hamming weights, intermediate and output are also independent of the message and of the **key** . Finally, the **cryptographically** processed message is output. External monitoring of the hardware device does not reveal useful information about the secret **key** .

INDEPENDENT CLAIMS are included for a balanced **cryptographic**

processing device, a method for performing a balanced **cryptographic** operation using the secret data, a method for reducing the amount of information available for detection by **monitoring** the device **power** consumption, a method for converting a definition of a computational device for **cryptography** using a secret **key** into a definition of a digital circuit and a method for converting a definition of a computational device for **cryptography** into a definition of software whose power consumption is balanced.

USE - For 'leaky' hardware elements, e.g. **smart cards** .

ADVANTAGE - The electromagnetic radiation leakage and power consumption of a device employing the method does not give any clue to the **cryptography** going on inside, making the device more **secure** .

DESCRIPTION OF DRAWING(S) - The figure shows an example CMOS integration of a leakless NAND gate.

pp; 39 DwgNo 6/8

Title Terms: COMPUTATION; METHOD; SECRET; **KEY** ; MESSAGE; BALANCE; LEAK; MINIMISE; SMART; CARD; **CRYPTOGRAPHIC** ; SYSTEM

Derwent Class: P85; T01; T04; U21; W01

International Patent Class (Main): G06F-001/24; G06F-011/30; G09C-001/12

File Segment: EPI; EngPI

12/5/29 **(Item 29 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

012766208 **Image available**
WPI Acc No: 1999-572336/199948
XRPX Acc No: N99-421759
Device to protect **microprocessor card against fraudulent analysis of operations performed by** measuring current **consumed**
Patent Assignee: GEMPLUS SCA (GEMP-N); GEMPLUS (GEMP-N)
Inventor: BENOIT O; FEYT N; NACCACHE D
Number of Countries: 025 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9949416	A1	19990930	WO 99FR583	A	19990316	199948	B
FR 2776410	A1	19990924	FR 983471	A	19980320	199948	
EP 1062633	A1	20001227	EP 99907717	A	19990316	200102	
			WO 99FR583	A	19990316		
CN 1288548	A	20010321	CN 99802033	A	19990316	200137	
JP 2002508549	W	20020319	WO 99FR583	A	19990316	200222	
			JP 2000538317	A	19990316		
EP 1062633	B1	20031217	EP 99907717	A	19990316	200404	
			WO 99FR583	A	19990316		
DE 69913667	E	20040129	DE 613667	A	19990316	200416	
			EP 99907717	A	19990316		
			WO 99FR583	A	19990316		
US 6698662	B1	20040302	WO 99FR583	A	19990316	200417	
			US 2000646564	A	20001218		

Priority Applications (No Type Date): FR 983471 A 19980320
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9949416	A1	F	18	G06K-019/073	
Designated States (National): CA CN IN JP SG US					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
FR 2776410	A1			G06K-019/073	
EP 1062633	A1	F		G06K-019/073	Based on patent WO 9949416
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
CN 1288548	A			G06K-019/073	
JP 2002508549	W		15	G06K-019/073	Based on patent WO 9949416
EP 1062633	B1	F		G06K-019/073	Based on patent WO 9949416
Designated States (Regional): DE ES FR GB IT					
DE 69913667	E			G06K-019/073	Based on patent EP 1062633
					Based on patent WO 9949416
US 6698662	B1			G06K-019/06	Based on patent WO 9949416

Abstract (Basic): WO 9949416 A1
NOVELTY - The microprocessor card has added a device (20), connected to the supply input, which modifies the current consumption of the card, by averaging, integration or adding of random values from a random signal generator (28) on the card. The technique can also be applied to masking of writing to EEPROM.
USE - **Security** of **smart cards** and EEPROM writing process.
ADVANTAGE - Prevents intruder determining **key** by **monitoring current** consumption of microprocessor on **smart card** as it executes its program. Uses a masking device to conceal the operations undertaken, while allowing the programmer free-choice in the rules of programming, which could be of the Octet Orientated type.
DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of the card
Current consumption modification device (20)
Random signal generator (28)
pp; 18 DwgNo 1/3
Title Terms: DEVICE; **PROTECT** ; MICROPROCESSOR; CARD; FRAUD; ANALYSE; OPERATE; PERFORMANCE; MEASURE; CURRENT; CONSUME
Derwent Class: T01; T04

International Patent Class (Main): G06K-019/06; G06K-019/073
International Patent Class (Additional): **G06F-012/14**
File Segment: EPI

12/5/38 (Item 38 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007367760 **Image available**
WPI Acc No: 1988-001695/198801
XRPX Acc No: N88-001335

Integrated circuits for storage and processing of information - uses internal configuration of storage transistors arranged so unprogrammed and cells appear to draw same current programmed

Patent Assignee: THOMSON COMPOSANTS (CSFC); EUROTECHNIQUE SA (EURO-N); THOMSON COMP MILITA (CSFC); THOMSON COMP MILI (THOH); THOMSON COMPOSANTS MILITAIRES (CSFC)
Inventor: FRUHAUF S; LISIMAQUE G
Number of Countries: 008 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 251853	A	19880107	EP 87401324	A	19870612	198801	B
FR 2600183	A	19871218				198807	
US 4813024	A	19890314	US 8762078	A	19870610	198913	
EP 251853	B	19920325	EP 87401324	A	19870612	199213	
DE 3777701	G	19920430				199219	
ES 2030085	T3	19921016	EP 87401324	A	19870612	199246	

Priority Applications (No Type Date): FR 868589 A 19860613
Cited Patents: FR 2311360; US 4211919; US 4295041
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 251853	A	F	8		
Designated States (Regional): CH DE ES FR GB IT LI					
US 4813024	A		6		
EP 251853	B		8		
Designated States (Regional): CH DE ES FR GB IT LI					
ES 2030085	T3			G06F-012/14	Based on patent EP 251853

Abstract (Basic): EP 251853 A

The ' **smart** ' **card** integrated circuit has a non-volatile programmable memory holding data on access authorisation. An input/output circuit (E/S) permits connection to a data transfer device and a processor (MP) connects input/ output and memory. The processor compares (COMP) access data with a code or **key** introduced through the input/output device.

Storage is caused in a memory zone of an error bit, or of an access bit in a second memory zone, depending on the correctness of the entered code. The second memory uses a single cell which, when activated, consumes the same current as an unprogrammed cell in the first memory zone.

ADVANTAGE - Provides **security** against fraudulent access by **current monitoring** to data by ensuring that access cell draws same current as virgin cell.

1/5

Title Terms: INTEGRATE; CIRCUIT; STORAGE; PROCESS; INFORMATION; INTERNAL; CONFIGURATION; STORAGE; TRANSISTOR; ARRANGE; SO; UNPROGRAMMED; CELL; APPEAR; DRAW; CURRENT; PROGRAM
Derwent Class: T01; T04; U14
International Patent Class (Main): **G06F-012/14**
International Patent Class (Additional): G06F-001/00; G06K-019/06; G07F-007/10; G11C-013/00
File Segment: EPI